Doc Code: AP.PRE.REQ

PTO/SB/33 (07-05)
Approved for use through xx/xx/200x. OMB 0651-00xx
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Docket Number (Optional): NAI1P492/03.028.01

I hereby certify that this correspondence is being e-filed with the USPTO

on September 17, 2007

Signature /Dana Chan/

Typed or printed name Dana Chan

Application Number	Filed
10/620,364	07/17/2003

First Named Inventor: Colin John Blamires

Art Unit	Examiner
2134	Simitoski, Michael J.

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a notice of appeal.

The review is requested for the reason(s) stated on the attached sheet(s).
Note: No more than five (5) pages may be provided.

I am the

- ☐ applicant/inventor.
- ☐ assignee of record of the entire interest. See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96)
- ☑ attorney or agent of record. Registration number 41,429
- ☐ attorney or agent acting under 37 CFR 1.34. Registration number if acting under 37 CFR 1.34 _____

/KEVINZILKA/
Signature

Kevin J. Zilka
Typed or printed name

408-971-2573
Telephone number

September 17, 2007
Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

☑ *Total of 1 forms are submitted.

REMARKS

The Examiner has not specifically rejected Claims 5, 9, 13, 17, 21, 25, and 31 under 35 U.S.C. 112. However, in the latest Office Action dated 5/15/2007, the Examiner has responded to applicant's arguments from the Amendment dated 03/12/2007.

Specifically, with respect to Claims 5, 9, 13, 17, 21, and 25, the Examiner has argued that "[t]he limitation recited that a firewall is disposed between the computer being controlled by the removable physical media and the remote computer appears to have no limiting effect on the removable physical media itself."

Applicant respectfully disagrees and asserts that applicant specifically claims a technique "wherein a firewall computer disposed between said computer and said remote computer is operable to block a connection between said computer and said remote computer other than said secure network connection," and that "said network support code is used to enable said computer to establish said secure network connection via said firewall computer to said remote computer," in the context claimed (see this or similar, but not necessarily identical language in the aforementioned independent claims - emphasis added). Thus, applicant's "firewall...," as claimed, does indeed add to the limitations of the claims as "said network support code is used to enable said computer to establish said secure network connection via said firewall computer to said remote computer" (emphasis added), in the context claimed by applicant.

Still yet, with respect to Claim 25, the Examiner has argued that "[certain] limitations are in question because the claim is directed to a server computer and the...limitations appear to provide no further components of the server." Applicant respectfully disagrees and asserts that, with respect to the claim limitations in question, applicant claims that the "computer is booted with a non-installed operating system ... [and that the] network support code is loaded for said computer ... [and] malware detection is performed upon said computer" (emphasis added), and that therefore such limitations do add to the server computer because "[the] server computer [is] connected by a network link to [the] computer" (emphasis added), in the context claimed by applicant. Additionally, with respect to the claim limitations in question, applicant clearly claims that "network support code is used to enable said computer to establish said secure network connection via said firewall to said server computer" (emphasis added), and that "malware detection is performed upon said computer using said one or more malware detection files,"

where the server "load[s] [the] one or more malware detection files to said computer," in the context claimed.

Further, with respect to Claim 31, the Examiner has argued that 'the limitation "wherein said remote computer logs said downloading of said one or more malware detection files by said computer" appears to have no effect on the claim because claim 1 is directed to a removable physical media which does not necessarily change as a result of the actions of a remote computer.' Applicant respectfully disagrees and asserts that applicant clearly claims "log[ging] said downloading of said one or more malware detection files by said computer," where "one or more malware detection files [are downloaded from the remote computer]," in the context claimed.

The Examiner has rejected Claims 1-3, 7-11, 15-19, 23-25, and 28-30 under 35 U.S.C. 103(a) as being unpatentable over Reinert et al. (U.S. Patent No. 6,347,375), in view of Yadav (U.S. Publication No. 2003/0149887), and further in view of "Network Security Essentials, Applications and Standards," by Stallings. Applicant respectfully disagrees with such rejection.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

With respect to the obviousness of combining the Reinert and Yadav references, the Examiner has argued that "it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Reinert [with Yadav] to connect to the remote computer via a secure connection." To the contrary, applicant respectfully asserts that it would not have been obvious to combine the teachings of the Reinert and Yadav references, especially in view of the vast evidence to the contrary.

Specifically, the Reinert reference teaches that "the present invention discloses a method and apparatus for providing up-to-date virus scanning of a local computer by a remote computer comprising those situations where the normal operating system of the local computer is not operable" (Col. 3, lines

44-48 - emphasis added). On the other hand, the Yadav reference teaches "[n]etwork intrusion detection [that] accurately identifies and takes into consideration currently running network applications by examining machine instructions embodying those applications" (Abstract, lines 1-4 - emphasis added).

If the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims *prima facie* obvious. *In re Ratti*, 270 F.2d 810, 123 USPQ 349 (CCPA 1959)

Combining a method where the normal operating system is not operable, as in Reinert, with an intrusion detection system that takes into consideration currently running network applications, as in Yadav, would require an impermissible change in the principle of operation of Reinert, contrary to *In re Ratti*. Thus, the Examiner's proposed combination is inappropriate. To this end, the first element of the *prima facie* case of obviousness has not been met.

More importantly, applicant also respectfully asserts that the third element of the *prima facie* case of obviousness has not been met by the prior art excerpts relied on by the Examiner. For example, with respect to the independent claims, the Examiner has relied on Col. 7, lines 4-5 and lines 65-67 from Reinert; paragraphs 0042-0044 from Yadav; pages 320-323, and the "private network" in Fig. 10.1(a) from Stallings to make a prior art showing of applicant's claimed technique "wherein said network support code is used to enable said computer to establish said secure network connection via said firewall computer to said remote computer" (see this or similar, but not necessarily identical language in the independent claims).

Applicant respectfully asserts that the excerpts from Reinert relied upon by the Examiner merely teach that "[i]f any viruses are detected, the user may then connect to the remote computer utilizing the communications program" (Col. 7, lines 4-5), and that "[i]f the local user desires to connect with the remote computer 54, a communications program is invoked by the local user to establish a communications connection" (Col. 7, lines 65-67 – emphasis added). Additionally, the excerpts from Yadav merely teach that "the SOC 270 and the NIDS may communicate over a virtual private network (VPN) 284, with its own encryption and security features, or use Secure Sockets Layer (SSL) to create a secure connection" (Paragraph 0044). Furthermore, the excerpts cited from Stallings only generally teach "FIREWALL DESIGN PRINCIPLES" (see page 320), which includes general information on "Firewall Characteristics" (see page 321) and "Types of Firewalls" (see page 322). Moreover, Fig. 10.1(a) from Stallings merely illustrates a "Packet-filtering router" between the "Internet" and the "Private network."

However, disclosing that a user may connect to a remote computer utilizing a communications program (see Reinert), utilizing a VPN or a SSL to create a secure connection (see Yadav), along with a general firewall description (see Stallings), fails to specifically teach that "network support code is used to enable said computer to establish said secure network connection via said firewall computer to said remote computer" (emphasis added), as claimed by applicant. Applicant respectfully asserts that only applicant teaches and claims the loading of network support code from removable physical media which specifically enables the secure network connection via the firewall, in the context claimed.

In addition, the Examiner has specifically argued that "[i]n light of [a]pplicant's [previous] amendments, the Stallings reference is submitted," and that "[a]s herein modified, the code [of Reinert] is also used to establish the secure connection via said firewall, as the packets must traverse the firewall for reception at the remote computer" (see page 5 of the Office Action dated 05/15/2007). Applicant respectfully disagrees and asserts that even in view of the improper combination of the Reinert, Yadav, and Stallings references, the proposed combination fails to teach or suggest that "said network support code is used to **enable** said computer to establish said secure network connection **via said firewall** computer to said remote computer" (emphasis added), in the context claimed by applicant, for at least the reasons noted above.

Applicant respectfully asserts that at least the first and third elements of the *prima facie* case of obviousness have not been met, since it would be *unobvious* to combine the references, as noted above, and the prior art excerpts, as relied upon by the Examiner, fail to teach or suggest all of the claim limitations, as noted above.

Applicant further notes that the prior art is also deficient with respect to the dependent claims. For example, with respect to Claim 29, the Examiner has relied on Col. 8, lines 14-16 and lines 25-31 from the Reinert reference to make a prior art showing of applicant's claimed technique "wherein said one or more malware detection files are determined based on said non-installed operating system."

Applicant respectfully asserts that the excerpts from Reinert relied upon by the Examiner merely teach that "a service program is downloaded from the remote computer 54 to the local computer 42" (Col. 8, lines 14-16 - emphasis added), and that "[d]ownloading the virus scanning software into the local computer memory 41 provides advantages ... because the virus scanning and virus repairing programs may be executed in the local computer memory" (Col.8, lines 25-29 – emphasis added). However, simply

disclosing that a program is downloaded from the remote computer to the local computer and may be executed in local memory, as in Reinert, fails to even suggest that "one or more malware detection files are determined based on said non-installed operating system" (emphasis added), as specifically claimed by applicant.

Additionally, with respect to Claim 30, the Examiner has relied on Col. 8, lines 20-35 from the Reinert reference to make a prior art showing of applicant's claimed technique "wherein said one or more malware detection files are determined based on a malware detection product." Specifically, the Examiner has argued that "the virus detection signature file is used by the virus scanning software utility program."

Applicant respectfully disagrees and asserts that the excerpt relied upon by the Examiner merely teaches that "[i]f the local computer 42 requests virus scanning services, a virus scanning software utility program is downloaded into the local computer memory 41 via communications hardware modems 58 and 40, respectively," and that "a complete up-to-date virus signature file is downloaded into the local computer memory 41" (Col. 8, lines 20-25).

However, downloading a virus scanning software utility program as well as a virus signature file, as in Reinert, fails to specifically suggest a technique "wherein said one or more malware detection files are determined based on a malware detection product" (emphasis added), as claimed by applicant. Moreover, asserting that "the virus detection signature file is used by the virus scanning software utility program," as argued by the Examiner, fails to suggest that "one or more malware detection files are determined based on a malware detection product" (emphasis added), as claimed by applicant.